Your Ref.: 066358.0102JP

Our Ref.: S-1181-1/002365

JAPANESE TRANSLATION OF PCT APPLICATION

International Patent Application No.

PCT/US99/07262

Date of International Application:

April 2, 1999

TITLE OF THE INVENTION

Multiple Transform Utilization and Applications for Secure Digital Watermarking

INVENTOR

SCOTT A. MOSKOWITZ

APPLICANT

SCOTT A. MOSKOWITZ

YUASA AND HARA

受領書

平成１２年１０月　２日
特　許　庁　長　官

識別番号　　１００００８９７０５
氏名（名称）　　社本　一夫　　殿
提出日　　平成１２年１０月　２日

以下の書類を受領しました。

項番	書類名	整理番号	受付番号	出願番号通知（事件の表示）
1	国内書面	002365	50001273422	PCT/US99/ 7262

以　上

【書類名】　国内書面

【整理番号】　002365

【提出日】　平成12年10月 2日

【あて先】　特許庁長官殿

【出願の表示】

【国際出願番号】　PCT/US99/07262

【出願の区分】　特許

【発明者】

【住所又は居所】　アメリカ合衆国フロリダ州３３１６０，マイアミ，コリンズ・アベニュー　１６７１１，ナンバー　２５０５

【氏名】　モスコウィッツ，スコット・エイ

【特許出願人】

【住所又は居所】　アメリカ合衆国フロリダ州３３１６０，マイアミ，コリンズ・アベニュー　１６７１１，ナンバー　２５０５

【氏名又は名称】　スコット・エイ・モスコウィッツ

【代理人】

【識別番号】　100089705

【住所又は居所】　東京都千代田区大手町二丁目２番１号　新大手町ビル２０６区　ユアサハラ法律特許事務所

【弁理士】

【氏名又は名称】　社本　一夫

【電話番号】　03-3270-6641

【選任した代理人】

【識別番号】　100071124

【弁理士】

【氏名又は名称】　今井　庄亮

【選任した代理人】

【識別番号】　100076691

【弁理士】

【氏名又は名称】　増井　忠弐

【選任した代理人】

【識別番号】　100075270

【弁理士】

【氏名又は名称】　小林　泰

【選任した代理人】

【識別番号】　100096013

【弁理士】

【氏名又は名称】　富田　博行

【選任した代理人】

【識別番号】　100087424

【弁理士】

【氏名又は名称】　大塚　就彦

【手数料の表示】

【予納台帳番号】　051806

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書の翻訳文　1

【物件名】　図面の翻訳文　1

【物件名】　要約書の翻訳文　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　安全なデジタル透かしのための複数の変換の利用及び適用

【特許請求の範囲】

【請求項１】　メッセージをデジタル情報に符号化する方法であって、前記デジタル情報は複数のデジタル・ブロックを含んでいる、方法において、

前記デジタル・ブロックのそれぞれをスペクトル変換を用いて周波数領域に変換するステップと、

前記変換されたデジタル・ブロックのそれぞれに対して、複数の周波数と関連する振幅とを識別するステップと、

前記デジタル・ブロックのそれぞれに対して、鍵からの基本マスクを用いて、前記識別された振幅の部分集合を選択するステップと、

畳み込みマスクを用いて発生された変換テーブルを用いて、前記メッセージからメッセージ情報を選ぶステップと、

前記選ばれたメッセージ情報に基づいて前記選択された振幅を変更することによって、前記選ばれたメッセージ情報を前記変換されたデジタル・ブロックのそれぞれに符号化するステップと、

を含むことを特徴とする方法。

【請求項２】　請求項１記載の方法において、前記変換するステップは、

高速フーリエ変換を用いて、前記デジタル・ブロックのそれぞれを前記周波数領域に変換するステップを含むことを特徴とする方法。

【請求項３】　請求項２記載の方法において、前記デジタル情報は、画像を形成する複数のカラー・チャネルにおけるピクセルを含み、前記デジタル・ブロックのそれぞれは、前記カラー・チャネルの１つにおけるピクセル領域を表すことを特徴とする方法。

【請求項４】　請求項１記載の方法において、前記デジタル情報はオーディオ情報を含むことを特徴とする方法。

【請求項５】　請求項２記載の方法において、前記識別するステップは、

前記変換されたデジタル・ブロックのそれぞれに対して最大の値を有する所定の数の振幅を識別するステップを含むことを特徴とする方法。

【請求項６】　請求項２記載の方法において、前記選ばれたメッセージ情報はメッセージ・ビットであり、前記符号化するステップは、

前記メッセージ・ビットが真である場合には強度率を用いて前記選択された振幅を減少させ、前記メッセージ・ビットが偽である場合には前記選択された振幅を減少させないことによって、前記選ばれたメッセージ・ビットを前記変換されたデジタル・ブロックのそれぞれに符号化するステップを含むことを特徴とする方法。

【請求項７】　請求項６記載の方法において、前記強度率はユーザによって定義されることを特徴とする方法。

【請求項８】　請求項２記載の方法において、前記選択された振幅と関連する周波数とのそれぞれを前記鍵に記憶するステップを更に含むことを特徴とする方法。

【請求項９】　請求項２記載の方法において、前記デジタル情報の基準部分集合を前記鍵に記憶するステップを更に含むことを特徴とする方法。

【請求項１０】　請求項２記載の方法において、前記デジタル情報は画像を形成するピクセルを含んでおり、更に、

前記ピクセルの基準部分集合を前記鍵にセーブするステップと、

前記画像の元の寸法を前記鍵に記憶するステップと、

を含むことを特徴とする方法。

【請求項１１】　請求項１記載の方法において、前記デジタル情報はオーディオ情報を含んでおり、更に、

オーディオ情報の基準部分集合を前記鍵にセーブするステップと、

前記オーディオ情報の元の寸法を前記鍵に記憶するステップと、

を含むことを特徴とする方法。

【請求項１２】　請求項１０記載の方法において、ピクセルの前記基準部分集合は前記画像におけるピクセルの線を形成することを特徴とする方法。

【請求項１３】　請求項１１記載の方法において、オーディオ情報の前記基準部分集合は振幅設定を含むことを特徴とする方法。

【請求項１４】　請求項８記載の方法において、前記画像は矩形であり、ピ

クセルの前記基準部分集合は前記矩形の対角線を形成することを特徴とする方法。

【請求項１５】　請求項２記載の方法において、

所定の鍵が前記符号化されたメッセージ情報を復号化することを要求するステップを更に含むことを特徴とする方法。

【請求項１６】　請求項２記載の方法において、

公開鍵の対が前記符号化されたメッセージ情報を復号化することを要求するステップを更に含むことを特徴とする方法。

【請求項１７】　請求項２記載の方法において、

前記メッセージに対する元のハッシュ値を計算するステップと、

前記元のハッシュ値を前記鍵に記憶するステップと、

を更に含むことを特徴とする方法。

【請求項１８】　鍵を用いてでる情報をデスケーリングする方法であって、

前記デジタル情報の元の寸法を前記鍵から決定するステップと、

前記デジタル情報を前記元の寸法にスケーリングするステップと、

情報の基準部分集合を前記鍵から取得するステップと、

前記基準部分集合を前記スケーリングされたデジタル情報における対応する情報と比較するステップと、

を含むことを特徴とする方法。

【請求項１９】　請求項１８記載の方法において、デスケーリングされる前記デジタル情報はデジタル画像であり、前記鍵から情報の基準部分集合を取得するステップは前記鍵からピクセルの基準部分集合を取得するステップを含むことを特徴とする方法。

【請求項２０】　請求項１８記載の方法において、デスケーリングされる前記デジタル情報はオーディオ・デジタル情報であり、前記鍵から情報の基準部分集合を取得するステップは前記鍵からオーディオ情報の基準部分集合を取得するステップを含むことを特徴とする方法。

【請求項２１】　請求項１９記載の方法において、前記比較するステップは前記比較に基づいて第１の適合する値を決定し、この方法は、更に、

前記スケーリングされたデジタル画像をパッド・ピクセルのエリアを用いてパディングするステップと、

ピクセルの前記基準部分集合を前記パディングされた画像における対応するピクセルと再度比較して第２の適合する値を決定するステップと、

を含むことを特徴とする方法。

【請求項２２】　請求項２０記載の方法において、パッド・ピクセルの前記エリアは、単一のピクセルのローであることを特徴とする方法。

【請求項２３】　請求項２０記載の方法において、パッド・ピクセルの前記エリアは、単一のピクセルのコラムであることを特徴とする方法。

【請求項２４】　請求項２０記載の方法において、前記パディング及び再度比較するステップは複数回実行されることを特徴とする方法。

【請求項２５】　請求項２０記載の方法において、前記決定された適合する値の中で最良の適合する値を選び、前記デジタル画像を元のサイズに回復し、前記最良の適合する値と関連する任意のパッド・ピクセルを含むステップを更に含むことを特徴とする方法。

【請求項２６】　所定の鍵を用いて符号化されたデジタル情報からメッセージを抽出する方法であって、

前記所定の鍵を用いて、前記符号化されたデジタル情報を複数のデジタル・ブロックを含むデジタル情報に復号化するステップと、

スペクトル変換を用いて、前記デジタル・ブロックのそれぞれを周波数領域に変換するステップと、

前記変換されたデジタル・ブロックのそれぞれに対して、複数の周波数と関連する振幅とを識別するステップと、

前記鍵からの基本マスクを用いて、前記変換されたデジタル・ブロックのそれぞれに対して、前記識別された振幅の部分集合を選択するステップと、

前記選択された振幅と前記所定の鍵に記憶された元の振幅とを比較し、符号化されたメッセージ情報の位置を決定するステップと、

前記符号化されたメッセージ情報と逆変換テーブルとを用いて、前記メッセージをアセンブルするステップと、

を含むことを特徴とする方法。

【請求項２７】　請求項２６記載の方法において、前記変換するステップは、

高速フーリエ変換を用いて、前記デジタル・ブロックのそれぞれを周波数領域に変換するステップを含むことを特徴とする方法。

【請求項２８】　請求項２７記載の方法において、

前記アセンブルされたメッセージに対するハッシュ値を計算するステップと、

前記計算されたハッシュ値を前記所定の鍵の中の元のハッシュ値と比較するステップと、

を更に含むことを特徴とする方法。

【請求項２９】　鍵を用いてデジタル信号をデスケーリングする方法であって、

前記鍵から前記デジタル信号の元の寸法を決定するステップと、

前記デジタル信号を前記元の寸法にスケーリングするステップと、

前記鍵から基準信号部分を取得するステップと、

前記基準信号部分を前記スケーリングされた信号における対応する信号部分と比較するステップと、

を含むことを特徴とする方法。

【請求項３０】　デジタル信号を保護する方法であって、

伝達関数ベースのマスク・セットと元のデジタル信号のオフセット座標値とから構成される所定の鍵を作成するステップと、

前記デジタル信号を前記所定の鍵を用いて符号化するステップと、

を含むことを特徴とする方法。

【請求項３１】　請求項３０記載の方法において、前記デジタル信号は連続的なアナログ波形を表すことを特徴とする方法。

【請求項３２】　請求項３０記載の方法において、前記所定の鍵は複数のマスク・セットを含むことを特徴とする方法。

【請求項３３】　請求項３０記載の方法において、前記マスク・セットは、公開鍵と秘密鍵とを含む鍵の対によって暗号化されることを特徴とする方法。

【請求項３４】　請求項３０記載の方法において、

デジタル透かし技術を用いて前記デジタル信号に関する権利者、使用又はそれ以外の情報を識別する情報を前記デジタル信号の中に符号化するステップを更に含むことを特徴とする方法。

【請求項３５】　請求項３０記載の方法において、前記デジタル信号は静止画像、オーディオ又はビデオを表すことを特徴とする方法。

【請求項３６】　請求項３０記載の方法において、

ランダム又は疑似ランダムな一連のビットを有する１つ又は複数のマスクを含むマスク・セットを選択するステップと、

前記マスク・セットを、前記伝達関数ベースのマスク・セットの開始において有効化するステップと、

を更に含むことを特徴とする方法。

【請求項３７】　請求項３６記載の方法において、前記有効化するステップは、

前記伝達関数ベースのマスク・セットの開始において計算されたハッシュ値を前記ハッシュ値の所定の伝達関数と比較するステップを含むことを特徴とする方法。

【請求項３８】　請求項３６記載の方法において、前記有効化するステップは、

前記伝達関数ベースのマスク・セットの開始におけるデジタル署名を前記デジタル署名の所定の伝達関数と比較するステップを含むことを特徴とする方法。

【請求項３９】　請求項３６記載の方法において、

デジタル透かし技術を用いて前記デジタル信号に関する権利者、使用又はそれ以外の情報を識別する情報を前記デジタル信号の中に埋め込むステップを更に含み、

前記有効化するステップは、前記埋め込まれた情報の有効化に依存することを特徴とする方法。

【請求項４０】　請求項３０記載の方法において、

前記デジタル信号においてキャリア信号データの安全な一方向ハッシュ関数を

計算するステップを更に含んでおり、前記ハッシュ関数は、前記伝達関数ベースのマスク・セットを搬送する目的で前記キャリア信号の中に導入された変化を感知しないことを特徴とする方法。

【請求項４１】　デジタル信号を保護する方法であって、

伝達関数ベースのマスク・セットと元のデジタル信号のオフセット座標値とで構成された所定の鍵を作成するステップと、

正しい伝達関数ベースのマスク・セットを含む前記所定の鍵を前記データの再生の間に認証するステップと、

前記データの再生を測定してコンテンツをモニタし、前記デジタル信号が変更されたかどうかを判断するステップと、

を含むことを特徴とする方法。

【請求項４２】　請求項３０記載の方法において、前記デジタル信号はビット・ストリームであり、この方法は、更に、

符号化のために用いられ、ランダム基本マスクと、ランダム畳み込みマスクと、メッセージ・デリミタのランダム開始とを含む複数のマスクを発生するステップと、

符号化されるメッセージ・ビット・ストリームを発生するステップと、

前記メッセージ・ビット・ストリームと、ステガ・サイファ・マップ真理テーブルと、前記基本マスクと、前記畳み込みマスクと、メッセージ・デリミタの前記開始とをメモリにロードするステップと、

基本マスク・インデクスと、畳み込みマスク・インデクスと、メッセージ・ビット・インデクスとの状態を初期化するステップと、

前記メッセージ・ビット・ストリームにおける全ビット数と等しくなるようにメッセージ・サイズを設定するステップと、

を含むことを特徴とする方法。

【請求項４３】　請求項４２記載の方法において、前記デジタル情報は複数のウィンドウを有しており、この方法は、更に、

サンプル・ストリームにおけるどのウィンドウの上で前記メッセージが符号化されるかを計算するステップと、

前記計算されたウィンドウにおける情報の安全な一方向ハッシュ関数を計算するステップであって、前記ハッシュ関数はステガ・サイファによって導かれるサンプルにおける変化を感知しないハッシュ値を発生する、ステップと、

データの符号化されたストリームにおける前記計算されたハッシュ値を符号化するステップと、

を含むことを特徴とする方法。

【請求項４４】　請求項４０記載の方法において、前記選択するステップは、

ランダム・タイピングにおけるキーボード・レイテンシ期間から導かれた一連のランダム・ビットを収集するステップと、

初期の一連のランダム・ビットをＭＤ５アルゴリズムを介して処理するステップと、

前記ＭＤ処理の結果を用いて、トリプルＤＥＳ暗号化ループを供給し、各サイクルの後のそれぞれの結果の最下位ビットを抽出するステップと、

前記トリプルＤＥＳ出力ビットをランダムな一連のビットの中に連結するステップと、

を含むことを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル情報の保護に関する。更に詳しくは、本発明は、安全なデジタル透かしのための複数の変換の利用及び適用に関する。

【０００２】

【関連出願への相互参照】

本発明は、１９９６年１月１７日に出願された米国特許出願第０８／５８７，９４３号"Method for Stega-Cipher Protection of Computer Code"に基づいて優先権を主張している。この米国特許出願の開示のすべてを、本出願において援用する。

【０００３】

【従来の技術】

商業的に価値のある情報が「デジタル」形式で制作され記憶されることが増加している。例えば、音楽、写真及び画像のすべてが、１及び０などの一連の数として記憶され伝送されることが可能である。デジタル技術によると、元の情報を非常に正確に再生することができる。しかし、不運なことに、デジタル技術によると、その持ち主の許可を得ることなく、情報を容易にコピーすることもできるのである。

【０００４】

デジタル透かし（電子透かし、digital watermark）は、デジタル化されたマルチメディア・コンテンツの制作者（creators）と出版業者（publishers）とがコンテンツのローカルで安全な識別及び認証を要求する収束点に存在している。侵害行為（piracy）は貴重なデジタル情報の流通を損なう方向に作用するから、そのような作品のコピーや二次的（derivative）なコピーに対する責任を確立することが重要である。デジタル透かしシステムの目的は、基礎となるコンテンツ信号の中に、ほとんど又は全く痕跡を残すことなく、そして知覚可能であることが標準となるように、与えられた１つ又は複数の情報信号を挿入することである。その際に、基礎となる信号における符号化レベルと位置感度（location sensitivity）とを最大化することにより、この透かしを除去しようと試みるとコンテンツ信号に強制的に損傷が生じるようになっている。「マスタ」、ステレオ、ＮＴＳＣ（National Television Standards Committee）ビデオ、オーディオ・テープ又はコンパクト・ディスクであるかどうかなど、マルチメディア・コンテンツの様々な形態を考慮すると、質に関する寛容度は、個人ごとに変動し、そのコンテンツの基礎となる商業的及び美的な価値に影響を与える。従って、著作権、所有権（ownership right）、購入者情報又はこれらの何らかの組合せや関連データをそのコンテンツの中に結合させ、それにより、それが商業的であってもそれ以外の態様であっても認証されていない流通がそれ以後なされる場合には、そのコンテンツが損傷を受け、従って、その価値が低下するようにすることが望ましい。デジタル透かしは、このような関心の多くに向けられたものであり、この技術分野における研究は、これまでに、極めて堅固で安全な実現に対する豊かな

基礎を提供してきている。

【０００５】

特に関心が向けられているのは、コンテンツのデジタル化された「作品」（piece）の価値とそのコンテンツに値する「保護」を提供するためのコストとのバランスである。現実の世界における経済行動と並行するように、商業銀行の安全性（セキュリティ）を知覚できるからといって、銀行預金をするのに要する費用及び時間のために、人々は直ちに現金を銀行に預金するということにはならない。ほとんどの個人にとっては、１００米ドルをもっているからといって、それを財布にしまっておく以上の保護が必要とされることはない。また、ワールド・ワイド・ウェブ（WWW）すなわちウェブが存在するからといって、オーディオや、静止画像等の媒体のようなデジタル化することができる媒体に対して価値が創造されたことを意味しない。ウェブは、単に、情報交換のための媒体であり、コンテンツの商業的な価値を決定することはない。しかし、媒体を交換するためにウェブを用いることにより、その価値を決定するのに役立つ情報が提供されるため、デジタル化されたコンテンツに対する責任が要求される。デジタル透かしは、このプロセスにおけるツール（道具）であって、著作権などの法的権利に関するより公的な課題を確立するそれ以外の機構に代わるものではないことに注意してほしい。例えば、デジタル透かしは、コンテンツの価値を判断する際の「履歴平均」（historical average）アプローチに代わるものではない。これは、コンテンツの知覚された価値だけに基づいて購入をしようとする個人の市場（マーケット）のことである。例えば、インターネット又はそれ以外の任意の電子的な交換手段を介して写真が流通しても、その写真の基礎的な価値が増加することは必ずしもない。しかし、そのような形式の「放送」によってより大きな観客に到達する機会が生じることは、「潜在的」により大きな市場に基づく価値を生じさせる望ましい機構でありうる。この決定は、当該権利者のみが唯一なすことができる。

【０００６】

実際、多くの場合に、コンテンツの時間的な価値に依存して、アクセスが適切に制御されていない場合には、価値が現実に低下することがありうる。月刊誌と

して販売されている雑誌の場合には、その雑誌が販売されている期間を超えて、その雑誌に掲載されている写真の価値を評価することは困難である。コンパクト・ディスクの価値に関しても、同様な時間に関する変動要素があるし、デジタル化されたオーディオ信号のパッケージングとパッケージを伴わない電子的な交換とのような有形的な変動要素もある。インターネットは、単に、消費者により迅速に到達する手段を提供するだけであって、それ以外の「市場に基づく」価値に取って代わるものではない。デジタル透かしは、適切に実現されるのであれば、権利者の決定に関する必要な層を追加することになり、デジタル透かしが「証明可能な程度に安全」（provably secure）であるときには、価値を決定し評価する際に大いに役立つ。本発明は、デジタル透かし技術の改良であり、現実世界における商品の真偽判定方法と類似する態様で、デジタル化されたコンテンツを「改ざん不能」（tamper-proof）にする手段を与える。

【０００７】

デジタル透かし技術における一般的な弱点は、透かしを実現する方法に関する。ほとんどのアプローチにおいて、保護されるべき作品の制作者ではなくデジタル透かしを実現する者に、検出及び復号制御に関して依存している。様々な透かし技術が有するこの基本的側面のために、第三者がそのようなデジタル透かしの実現を成功裏に利用する際には、この技術の改良に対する適切な経済的インセンティブが失われる。特定の形式の利用がいったんなされると、それ以後の透かしの検出が曖昧になる。そして、それ以後の時点において同じ透かしプロセスを用いた符号化を成功であると見なすことになる。

【０００８】

安全なデジタル透かしのいくつかの実現例がこの基本的な制御の課題に取り組んでおり、「キー・ベース」（key-based）のアプローチの基礎を形成している。これらは、以下の米国特許及び出願中の米国特許出願がカバーしている。すなわち、"Steganographic Method and Device"と題する米国特許第５，６１３，００４号及びそれから生じた米国特許出願第０８／７７５，２１６号；"Human Assisted Random Key Generation and Application for Digital Watermark System"と題する米国特許出願第０８／５８７，９４４号；"Method for Stega-Cipher

Protection of Computer Code"と題する米国特許出願第０８／５８７，９４３号；"Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data"と題する米国特許出願第０８／６７７，４３５号；及び"Z-Transform Implementation of Digital Watermarks"と題する米国特許出願第０８／７７２，２２２号である。これらの米国特許及び米国特許出願における開示内容は本出願において援用する。公開鍵暗号システムは、米国特許第４，２００，７７０号、第４，２１８，５８２号、第４，４０５，８２９号及び第４，４２４，４１４号に記載されている。これらの米国特許における開示内容は、本出願において援用する。

【０００９】

これらのデジタル透かしによるセキュリティ方法を改良することによって、複数の変換を用い、信号特性を操作し、必要な関係を符号化及び復号化動作に用いられるマスク・セットすなわち「鍵」に適用することが、これらの方法の最適化された組合せとして考察される。透かしの符号化は、符号化アルゴリズムにおいて用いられる変換に関して最終的にほんの僅かに異なるが、公開された分散型のアーキテクチャというより大きな課題によって、抹消しようとする試みに打ち勝つ、より堅固なアプローチが要求され、更には、透かしの検出を不可能にする手段が要求される。これらの「攻撃」は、計算論的に比較すると、正反対な態様（diametrically）で関連している。例えば、クロッピング（cropping）とスケーリング（scaling）とは、信号処理の向きが異なり、結果的には特定の透かしアプローチを脆弱化する可能性があるが、すべての透かしアプローチについてはそういうことはない。

【００１０】

ブロック・ベース又は全体のデータ・セット変換のいずれかを用いて符号化を行う現時点で利用できるアプローチは、必ず、空間領域又は周波数領域のどちらか一方においてデータを符号化するが、両方の領域においてそうすることは決してない。同時的なクロッピング及びスケーリングは、空間及び周波数領域に影響し、それによって、使用可能な透かしシステムのほとんどを曖昧にする。複数の操作を生き延びる能力は、透かしの入れられた媒体のセキュリティを確実にしよ

うとしている者にとっては明確な利点である。本発明は、鍵ベースのアプローチを用いて既存の透かしを改良することを目指している。その際に、それ以後に透かしが入れられるコンテンツを権利者やコンテンツ制作者がより広く制御できるようにする。

【００１１】

現時点で利用可能な多くの静止画透かしアプリケーションは、鍵ベースの実現例とは根本的に異なっている。これらの製品としては、デジマーク（Digimarc）社やシグナム（Signum）社による製品があるが、これらの製品は、復号化動作に関してはオリジナルの画像との比較に完全に依存している透かしメッセージを符号化することによって、堅固（robust）な透かしを提供することを目指している。ブロックごとに実行される離散コサイン変換である変換のそれ以後の結果は、デジタル的に符号が付される。埋め込まれた透かしは、画像の知覚的な質とは全く関係がなく、従って、一般的に利用可能なデコーダの逆方向の適用が、攻撃の非常によい最初のラインとなる。同様にして、符号化プロセスは、第三者によって適用されることもありうる。これは、いくつかの堅固性のテストにおいて示されているように、或るプロセスを用いて他のプロセスを用いて透かしが入れられた画像の結果を符号化するものである。透かしを放棄しないこと（nonrepudiation）はできない。その理由は、デジマーク社とシグナム社とが、画像の権利に関するすべての登録の機関として機能しているからである。

【００１２】

攻撃の別のラインとして、エラーのない検出が困難又は不可能であるように追加されている高周波ノイズの一部を除去するローパス・フィルタがある。最終的には、単純なＪＰＥＧ変換の多くのテストがこのような透かしは生き延びることができないことを示す。その理由は、ＪＰＥＧが、透かしを入れるプロセスによって用いられる符号化変換と同じ変換に基づいているからである。これ以外の注意すべき実現例としては、例えば、ＮＥＣの研究者たちによって開発されたシグナファイ（Signafy）によるものなどがあるが、画像の全体の変換を実行することによって、透かしメッセージを符号化しているようである。このプロセスの目的は、画像の「候補となる」透かしビット又は領域をより一貫性をもって識別し

て、信号の知覚的に著しい領域において符号化を行うことである。そうであっても、シグナファイは、復号化を達成するのに、オリジナルの透かしの入れられていない画像に依存する。

【００１３】

これらの方法は、すべてが、透かしを比較的エラーのない態様で検出することを確実にするために、オリジナルの透かしの入れられていない画像に依然として依存している。ステガノグラフィック（steganographic）な方法では、復号化動作のためにその媒体のオリジナルな透かしの入れられていないコピーを用いることなく透かしのセキュリティを提供すると共に、ユーザに暗号化された鍵を用いて暗号的なセキュリティをも提供することが目的とされる。すなわち、符号化動作と復号化動作とのために、同じ鍵が用いられる。それぞれのユーザが非対称的な符号化及び復号化動作を実行するための公開／秘密鍵対を有するような公開鍵対を用いることもできる。公開鍵暗号に関する議論と暗号化に関する利点とは、広く文書化がなされている。公開鍵インフラストラクチャの利用可能性が増加していることは、証明可能なセキュリティを認識しうるということを示している。透かしの実現化がこのように鍵ベースであることにより、セキュリティについては鍵に依存することが可能であり、それによって、透かしメッセージと透かしの入れられたコンテンツとのセキュリティ及び認証に対する多層化（layered）されたアプローチが得られる。

【００１４】

これ以外の実現例が生き延びること（survivability）に対するに対する攻撃も容易に利用可能であることが知られている。透かしメッセージに対する興味深いネットワーク・ベースの攻撃も知られているが、これは、中央の登録サーバを騙して、画像が登録されている権利者とは別の誰かが権利を有していると想定させるものである。また、これによると、集中的な透かし技術は十分に堅固なものではなく、マルチメディア作品のデジタル化されたコピーの権利者に関する適切な確認を行うことはできないという懸念が現実のものとなる。

【００１５】

【発明が解決しようとする課題】

複数の変換を実行することに関する計算論的な要求は、静止画やオーディオなどのある種の媒体にとっては禁止されないのであるから、本発明は、復号化を実行するのにオリジナルの透かしの入れられていないコピーを必要とすることなしに、媒体に確実に透かしを入れる手段を提供することを目的とする。これらの変換は、コンテンツの観察者又は権利者に対して単純には明らかでない態様で実行することができる。しかし、これらの観察者や権利者は、透かしが依然として検出可能であると考えることができる。更に、特定の媒体のタイプが一般的に圧縮されている場合（ＪＰＥＧ、ＭＰＥＧなど）には、複数の変換を用いて、透かしを入れるプロセスに先立ってマスク・セットを適切に設定し、透かしの入れられた従って知覚された「安全」なコピーを未知の第三者に解放する前に、ユーザに生き残り可能性について警告することができる。本発明の結果は、透かしへのより現実的なアプローチであって、鍵の証明可能なセキュリティだけでなく媒体のタイプも考慮している。従って、電子商取引のためのより信頼性の高いモデルも可能である。

【００１６】

透かしを挿入するために最適化された「封筒」を作成し、デジタル的にサンプリングされたコンテンツに対する確実な責任を確立することにより、大きな透かしセキュリティの基礎が得られるが、これは、本発明の補助的な目的である。発生される所定の又はランダムな鍵は、隠された情報信号にアクセスするために不可欠な地図であるだけではなく、オリジナルな信号の部分集合であって、それにより、オリジナルな信号との比較が不要になる。これによって、デジタル透かしの全体的なセキュリティが向上する。

【００１７】

同時的なクロッピング及びスケーリングが生き延びること（生き残ること、survival）は、画像及びオーディオ透かしに関しては、困難である。というのは、そのような変換は、画像やオーディオの偶然的（inadvertent）な使用と、透かしへの意図的な攻撃とで共通だからである。対応の効果は、オーディオの場合にはるかに明らかであるが、広帯域の変動などのように狭い意味で「周波数ベース」である透かしは、作品の元の長さから「クロッピング」又はクリップされたオ

ーディオ・サンプルにおけるアライメントの問題を有している。スケーリングは、人間の聴覚系にとってはるかにより顕著であるが、僅かな変化が、消費者には明らかではないにもかかわらず、周波数だけのタイプの透かしに影響することがありうる。ほとんどが周波数ベースの埋め込み形信号処理である、利用可能なオーディオ透かしアプリケーションに対するはるかに大きな脅威は、時間ベースの変換であり、これには、オーディオ信号の時間ベースの圧縮及び解凍が含まれる。シグナファイは、広帯域ベースの透かしの例であり、ソラナ（Solana）テクノロジ、ＣＲＬ、ＢＢＮ、ＭＩＴなどによるアプリケーションも同様である。「空間領域」アプローチというのが、デジマルク、シグナム、ＡＲＩＳ、アービトロン（Arbitron）などによって開発された技術に対するより適切な名称である。興味深いことに、時間ベースのアプローチは、画像について考察される場合には、基本的には空間ベースのアプローチである。ピクセルは、「畳み込み的」（convolutional）である。これら間の差異は、周波数の広帯域化された（spread-spectrum-ed）領域は「あまりに」うまく定義されているために、埋め込まれた信号と同じサブバンドでのランダム・ノイズの過剰な符号化を受けることになるという点である。

【００１８】

ジョバンニ（Giovannni）は、現実の透かしに対して、ブロック・ベースのアプローチを用いる。しかし、それには、スケーリングされた画像をその元のスケールに回復させることができる画像認識が伴っている。この「デスケーリング」は、画像が復号化される前に適用される。他のシステムでは、元の画像を透かし入りの画像と「区別」して「デスケーリング」を行っている。デスケーリングが、あらゆる画像、オーディオ又はビデオ透かしの生き残りにとって固有の重要性を有していることは明らかである。明らかでないのは、区別の動作がセキュリティの見地から受け入れ可能であるか、ということである。更に、画像のユーザ又は制作者ではなく、透かし「機関」によって区別が実行されなければならない場合には、権利者は、元の透かしの入っていないコンテンツを支配できないことになる。符号化／復号化鍵／鍵の対の内部でマスク・セットを用いることとは別に、元の信号を用いなければならない。オリジナルは、検出及び復号化を実行する

のに必要であるが、以上で説明した攻撃に関しては、透かしの入れられたコンテンツに対する権利を明確に確立することは不可能である。

【００１９】

以上を鑑みると、以上で論じた課題を解決する安全なデジタル透かしのための複数の変換の利用及び適用に対する実質的な必要性が存在することを理解することができるであろう。

【００２０】

【課題を解決するための手段】

安全なデジタル透かしのための複数の変換の利用及び適用によってこの技術における短所は大幅に改善することができる。本発明の或る実施例では、保護されるべきデジタル情報におけるデジタル・ブロックは、高速フーリエ変換を用いて周波数領域に変換される。複数の周波数及び関連する振幅が、変換されたデジタル・ブロックのそれぞれに対して識別され、識別された振幅の部分集合が、鍵からの基本マスクを用いてデジタル・ブロックのそれぞれに対して選択される。メッセージ情報は、畳み込みマスクを用いて発生された変換テーブルを用いて、メッセージから選択される。選ばれたメッセージ情報は、選択されたメッセージ情報に基づいて選択される振幅を変化させることによって、変換されたデジタル・ブロックのそれぞれに符号化される。

【００２１】

以下で明らかになる本発明のこれらの及びそれ以外の効果及び特徴により、本発明の性質は、以下で行う本発明の詳細な説明と、冒頭の特許請求の範囲と、添付の図面とを参照することによって、より明確に理解することができるはずである。

【００２２】

【発明の実施の形態】

本発明の或る実施例によると、安全なデジタル透かしのために複数の変換が用いられる。周波数領域又は空間領域の変換を用いる透かしには２つのアプローチが存在する。すなわち、小さなブロックを用いる場合とデータ・セット全体を用いる場合とである。オーディオやビデオのような時間ベースの媒体に対しては、

小さな部分において作業するのが実際的である。というのは、ファイル全体では、サイズが数メガバイトにもなりうるからである。しかし、静止画については、ファイルははるかに小さいのが通常であり、１回の操作で変換することができる。２つのアプローチは、それぞれが、各自の利点を有している。ブロック・ベースの方法は、クロッピングに対する抵抗性を有する。クロッピング（cropping）というのは、信号の部分的な切り取り又は除去である。データは複数の小さな部分（piece）に記憶されるので、クロッピングは、単に、いくつかの部分が失われることを意味する。１つの完全な透かしを復号化するのに十分なブロックが残っている限り、クロッピングによって、その透かしが除去されることはない。しかし、ブロック・ベースのシステムは、スケーリングに弱い。アフィン・スケーリング（affine scaling）又は「収縮」（shrinking）などのスケーリングは、信号の高周波の損失につながる。ブロックのサイズが３２サンプルであり、データが２００％スケーリングされる場合には、関係のあるデータは、６４サンプルをカバーすることになる。しかし、デコーダは、依然として、データは３２サンプルにあると考えるので、透かしを適切に読み取るのに必要な空間の半分しか用いない。セット全体のアプローチは、逆の振る舞いを有する。このアプローチは、スケーリングを生き延びるのは非常に得意である。その理由は、このアプローチでは、データを全体として扱い、符号化の前にデータを特定のサイズにスケーリングするのが一般的であるからである。しかし、どのように小さなクロッピングであっても、変換のアライメントを混乱させ、透かしを曖昧にしてしまう可能性がある。

【００２３】

本発明を用いると、そして、これまでに開示されている材料を組み入れることによって、符号化鍵／鍵の対を用いて画像や歌やビデオを認証し、暗号による誤った肯定的な一致を排除し、オリジナルな透かしの入れられていない作品の代わりに第三者の権限を備えた登録を通じて著作権の通信を提供することが可能となる。

【００２４】

本発明は、従来技術に対する明らかな改良を提供するのであるが、元（オリジ

ナル）の信号の座標値を鍵の上にオフセットし、次にそれを用いてユーザ又は認証を受けた「鍵の持ち主」による復号化又は検出動作が行われることによって、過去に開示された内容に対する改良がなされる。このオフセットは、透かしが、成功裏に符号化されうるデータの量を、シャノンのノイズを含むチャネルの符号化定理に基づいて「運ばせる」（ペイロードさせる）ことができるコンテンツにおいて必要であり、これによって、透かしメッセージを有する信号の十分に不可視的な「飽和」が回避され、権利者が単一のメッセージを検出することが可能となる。例えば、或る画像が単一の１００ビットのメッセージ又は１２のＡＳＣＩＩ文字を運ぶのに十分なペイロードだけを有するというのも、全くありうることである。本発明の発明者によってテストがなされたオーディオでの実現例では、毎秒１０００ビットが、１６ビットの４４．１ｋＨｚのオーディオ信号において、不可聴的に符号化される。電子的に利用可能なほとんどの画像は、同じ「ペイロード」率を与えることができるほどに十分なデータを有していない。従って、クロッピング及びスケーリングが同時に生き延びることは画像の場合の方が、それに対応する商業的に利用可能なオーディオ又はビデオ・トラックの場合よりも困難であることになる。追加されるセキュリティの効果は、広帯域又は周波数のみのアプリケーションに基づく透かしシステムのランダマイザが制限されているほど、透かしデータのランダム値は、制限された信号帯域上で「ホッピング」することになり、また、鍵もまた、ランダムな態様でより効果的に符号化を行うのに用いられる暗号化された又はランダムなデータの独立なソースである、ということである。鍵は、実際に、ビット数で測定した場合に、透かしメッセージ自体よりも大きなランダム値を有しうる。透かしデコーダは、画像が、そのオリジナルのスケールに含まれていることを求められ、また、その「デスケーリング」された寸法に基づいてクロッピングされたかどうかを決定することができる。

【００２５】

コンテンツに透かしを入れそのコンテンツの流通を有効化するために鍵を要求するシステムの利点は明らかである。異なる情報を符号化するには異なる鍵を用いることができる。その際に、安全な一方向ハッシュ関数や、デジタル署名や、更には一時的パッド（one-time pads）でさえも鍵の中に組み入れることによっ

て、埋め込まれた信号を保護し、透かしの入れられた画像とその鍵／鍵の対を拒絶せずに有効化することができる。後に、これらの同じ鍵を用いて、埋め込まれたデジタル署名だけを後で有効化する、又は、デジタル透かしメッセージを完全に復号化する。コンテンツにデジタル透かしが入れられているということだけでなく、流通業者はそれ以外にはどのような機能も有していない鍵を用いてデジタル署名のチェックを実行することによって透かしの有効性をチェックしなければならないということも、出版業者は、容易に要求することができる。

【００２６】

安全なデジタル透かしが、いくらか論じられ始めている。レイトン（Leighton）は、米国特許第５，６６４，０１８号に、デジタル透かしにおける共謀的な攻撃（collusion attack）を防止する手段を記載している。しかし、レイトンは、記載されているセキュリティを現実的には提供できない可能性がある。例えば、透かし技術が線形であるような特定の場合には、「挿入封筒」又は「透かし空間」が矛盾なく定義されており（well-defined）、従って、認証を受けていないものによる共謀よりは複雑でない攻撃を受ける可能性がある。透かし符号化レベルにおける過剰符号化（over encoding）は、そのような線形の実現例における１つの単純な攻撃に過ぎない。レイトンによって無視された別の考慮として、商業的価値のあるコンテンツは、多くの場合に、既に透かしの入れられていない形態でいずれかの場所に既に存在しており、潜在的な侵害行為に容易にさらされる状態にあるので、どのようなタイプの共謀行為も不要であるということがある。この例として、コンパクト・ディスクやデジタル放送されたビデオなど多くがある。透かしデータの前処理を用いて埋め込まれた信号にデジタル署名をすることによって、共謀の成功を回避することができる可能性が大きい。透かしを入れる媒体に依存するが、非常に個別化された（granular）透かしアルゴリズムは、ベースラインとなる透かしが何らかの機能を有しているという予測よりも、デジタル的にサンプリングがなされるあらゆる媒体において共通な与えられた量子化人工物を、何か観測可能なものよりも低いレベルで成功裏に符号化できる可能性が高い。

【００２７】

更に、ここで開示されている「ベースライン」透かしは、かなり主観的なものである。これは、この技術分野のいずれかの場所で信号の「知覚的に意義のある」領域として説明されるだけである。すなわち、透かし関数の線形性を減少させる、又は、透かしの挿入を反転させることにより、「ベースライン」透かしを阿ｓくせいするのに要求される追加的な作業なしに同じ効果が得られるように思われる。実際、透かしアルゴリズムは、追加的なステップなしに、ターゲット挿入封筒又は領域を既に定義することができるべきである。更に、本発明の発明者によって既に開示されている出願では、透かしデータに加えて、利用可能な透かし領域の「ビット空間」又は符号化とは関係のないランダム・ノイズよりも少ないビットを符号化するように設定することにより、可能性のある攻撃やそれ以外の抹消の試みを混乱させることができる透かし技術が説明されている。「候補ビット」の領域は、任意の数の圧縮方式又は変換によって定義することができ、すべてのビットを符号化するすることは必要でない。更に、すべてのビットを符号化することは、符号化方式を知りながら領域を複製することができるものにとっては、現実的には、セキュリティ上の弱点として作用する可能性がある。やはり、セキュリティは、実際の透かしメッセージの外部にオフセットされていなければならず、それによって、真に堅固で安全な透かしの実現が得られるのである。

【００２８】

対照的に、本発明は、様々な暗号化プロトコルを用いて実現し、基礎となるシステムにおける信頼性及びセキュリティの両方を強化することができる。所定の鍵は、マスクの組として説明される。これらのマスクには、基本、畳み込み及びメッセージ・デリミタが含まれるが、メッセージのデジタル署名などの追加的な領域にも拡張することができる。これまでに開示されている技術では、これらのマスクの機能は、写像に対してだけ定義されていた。公開及び秘密鍵を鍵の対として用いて、鍵が危険にさらされることがない可能性を増加させることができる。符号化の前に、上述のマスクは、暗号的な見地から安全なランダム発生プロセスによって発生される。ＤＥＳなどのブロック暗号は、十分にランダムなシード値（seed value）と組み合わされて、暗号的に安全なランダム・ビット発生器をエミュレートする。これらの鍵は、考察しているサンプル・ストリームにそれら

を一致させる情報と共にデータベースにセーブされ、デスクランブリング（スクランブル解除）や後の検出又は復号化動作に用いられる。

【００２９】

これらの同じ暗号化プロトコルを、スクランブルされていない状態でストリームされたコンテンツを正しく表示又は再生するために認証された鍵を要求するストリームされたコンテンツを管理する際に、本発明の実施例と組み合わせることができる。デジタル透かしの場合と同様に、対称的又は非対称的な公開鍵の対が、様々な実現例において用いられる。更に、真正の鍵の対を維持する認証機関に対する必要性も、対称的な鍵の実現例以上のセキュリティを得るためには、伝送の際のセキュリティを考える際には考慮すべき問題となる。

【００３０】

次に、本発明によるデジタル情報保護システムの或る実施例を説明する。ここで添付の図面を参照するが、同じ要素については、複数の図面にわたって同じ参照番号が付されている。図１には、本発明の実施例によるデジタル情報符号化方法のブロック流れ図が図解されている。１つの画像が「ブロック」ごとに処理されるのであるが、ここで、各ブロックは、例えば、単色チャネルにおける３２Ｘ３２のピクセル領域である。ステップ１１０では、各ブロックが、スペクトル変換又は高速フーリエ変換（ＦＦＴ）を用いて、周波数領域に変換される。ステップ１２０及び１３０において、最大の３２の振幅が識別され、これら３２の中の部分集合が、鍵からの基本マスクを用いて選択される。次に、１メッセージ・ビットが、ステップ１４０及び１５０において各ブロックの中に符号化される。このビットは、畳み込みマスクを用いて発生された変換テーブルを用いてメッセージから選ばれる。このビットが真である場合には、選択された振幅は、ユーザによって定義された強度率（strength fraction）だけ減少される。ビットが偽である場合には、振幅は不変である。

【００３１】

選択された振幅と周波数とは、それぞれが、鍵の中に記憶される。すべての画像が処理された後で、ピクセルの対角線方向のストライプが鍵にセーブされる。このストライプは、例えば、左上の角で開始して、画像を通って４５度の角度で

進むことができる。画像の元の寸法も、鍵に記憶される。

【００３２】

図２は、本発明の実施例によるデジタル情報デスケーリング方法のブロック流れ図である。画像が復号化のために選ばれると、最初に、クロッピング及び／又はスケーリングがなされているかどうかがチェックされる。されている場合には、画像は、ステップ２１０において、元の寸法にスケーリングされる。結果的に得られる「ストライプ」すなわちピクセルの対角線は、ステップ２２０において、鍵に記憶されているストライプとの適合が調べられる。適合がそれ以前の最良の適合よりも優れている場合には、スケールがステップ２３０及び２４０においてセーブされる。望むのであれば、例えば、ステップ２６０において、ゼロ・ピクセルの単一のロー又はコラムを用いて、画像をパディングすることができる。そして、このプロセスを反復して、適合が改善するかどうかを見ることができる。

【００３３】

ステップ２５０において完全な適合が見出される場合には、プロセスは終了する。完全な適合が得られない場合には、ユーザによって設定されるクロップ「半径」まで、プロセスが継続される。例えば、クロップ半径が４である場合には、画像を、４つのロー及び／又は４つのコラムまでパディングすることができる。ゼロによって置き換えられた任意のクロッピングされた領域を用いて、最良の適合が選ばれ、画像は、園もとの寸法まで回復される。

【００３４】

情報は、いったんデスケーリングされると、図３に示されている本発明の実施例に従って復号化される。復号化は、符号化の逆プロセスである。復号化された振幅は、鍵に記憶されたものと比較され、ステップ３１０及び３２０において、符号化されたビットの位置が決定される。メッセージは、ステップ３３０において、逆変換テーブルを用いてアセンブルされる。次に、ステップ３４０では、メッセージはハッシュ化され、このハッシュが元のメッセージのハッシュと比較される。元のハッシュは、符号化の間に鍵に記憶される。ハッシュが一致する場合には、メッセージは有効であると宣言され、ステップ３５０においてユーザに与

えられる。

【００３５】

この出願においては様々な実施例が特に図解され説明されているが、本発明の修正及び変形は、以上の説明によってカバーされ、本発明の精神と意図された範囲とから逸脱することなく、冒頭の特許請求の範囲に含まれる。更に、オーディオ及びビデオ・コンテンツに対して、時間ベースの信号操作や振幅及びピッチ動作のために、同様の動作が適用された。透かしの入れられていないオリジナルを用いることなくデスケーリング又はそれ以外の態様で迅速に差異を判断できる能力が、安全なデジタル透かしにとっては、固有の重要性を有している。デジタル化されたコンテンツはネットワークを介して交換されるので、拒絶されないことと第三者による認証とを保証することも重要である。

【図面の簡単な説明】

【図１】

本発明の或る実施例によるデジタル情報の符号化方法のブロック流れ図である。

【図２】

本発明の或る実施例によるデジタル情報のデスケーリング方法のブロック流れ図である。

【図３】

本発明の或る実施例によるデジタル情報の復号化方法のブロック流れ図である。

【書類名】　図面

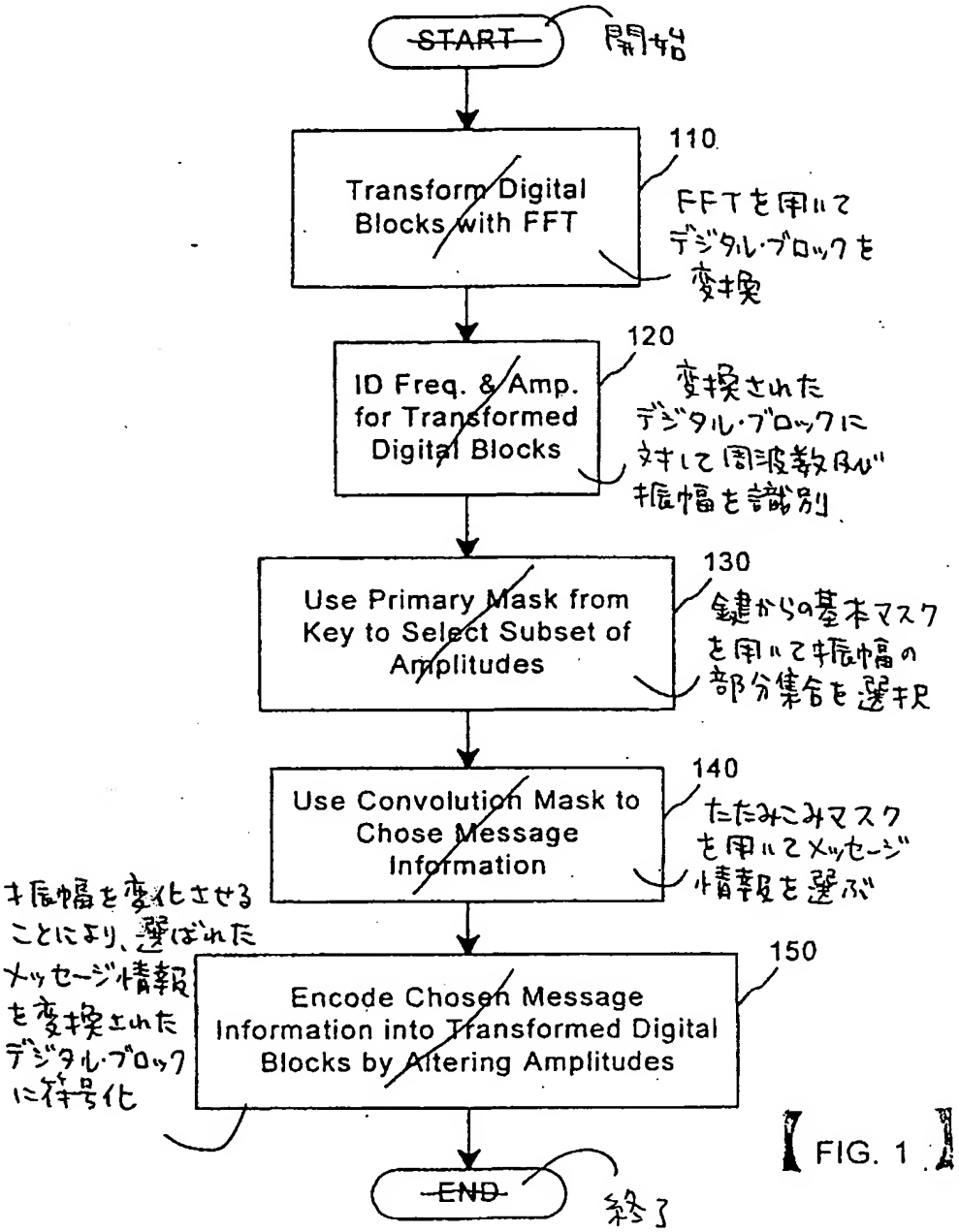

START
開始
110
Transform Digital Blocks with FFT
FFTを用いてデジタル・ブロックを変換
120
ID Freq. & Amp. for Transformed Digital Blocks
変換されたデジタル・ブロックに対して周波数及び振幅を識別
130
Use Primary Mask from Key to Select Subset of Amplitudes
鍵からの基本マスクを用いて振幅の部分集合を選択
140
Use Convolution Mask to Chose Message Information
たたみこみマスクを用いてメッセージ情報を選ぶ
振幅を変化させることにより、選ばれたメッセージ情報を変換されたデジタル・ブロックに符号化
150
Encode Chosen Message Information into Transformed Digital Blocks by Altering Amplitudes
END
終了

FIG. 1

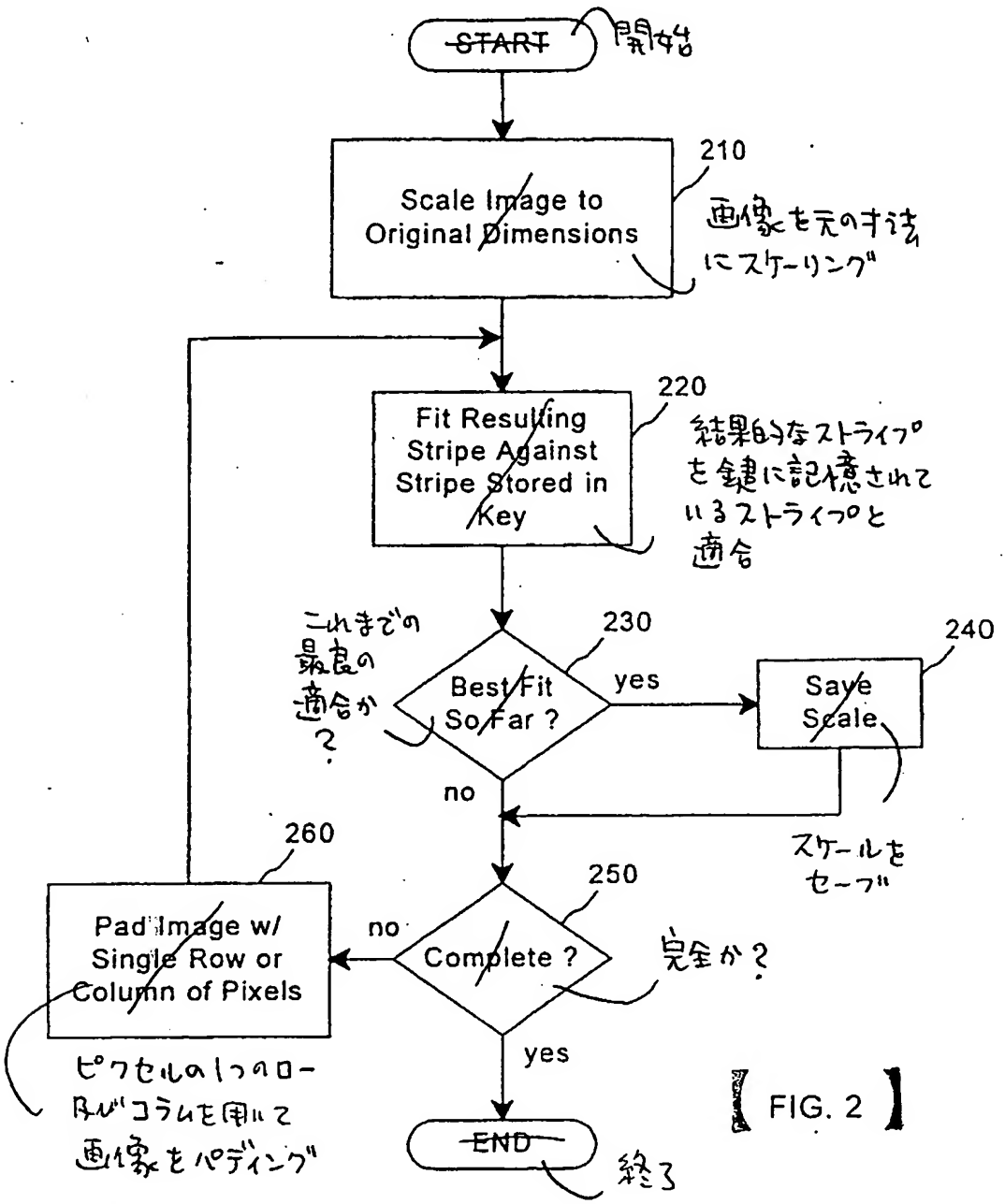
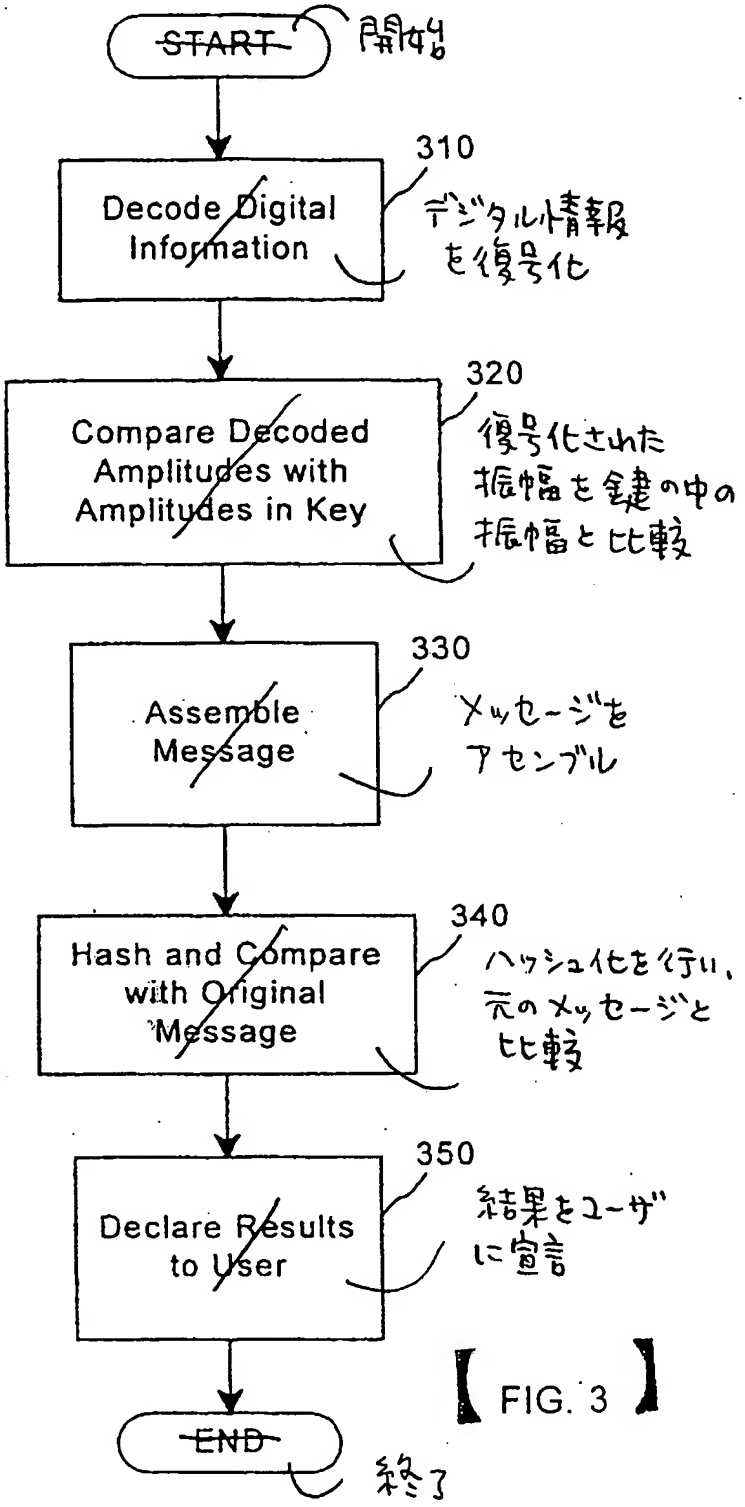

START
開始
Scale Image to Original Dimensions
210
画像を元の寸法にスケーリング
Fit Resulting Stripe Against Stripe Stored in Key
220
結果的なストライプを鍵に記憶されているストライプと適合
これまでの最良の適合か？
Best Fit So Far ?
230
yes
Save Scale
240
スケールをセーブ
no
Pad Image w/ Single Row or Column of Pixels
260
ピクセルの1つのロー及びコラムを用いて画像をパディング
no
Complete ?
250
完全か？
yes
END
終了

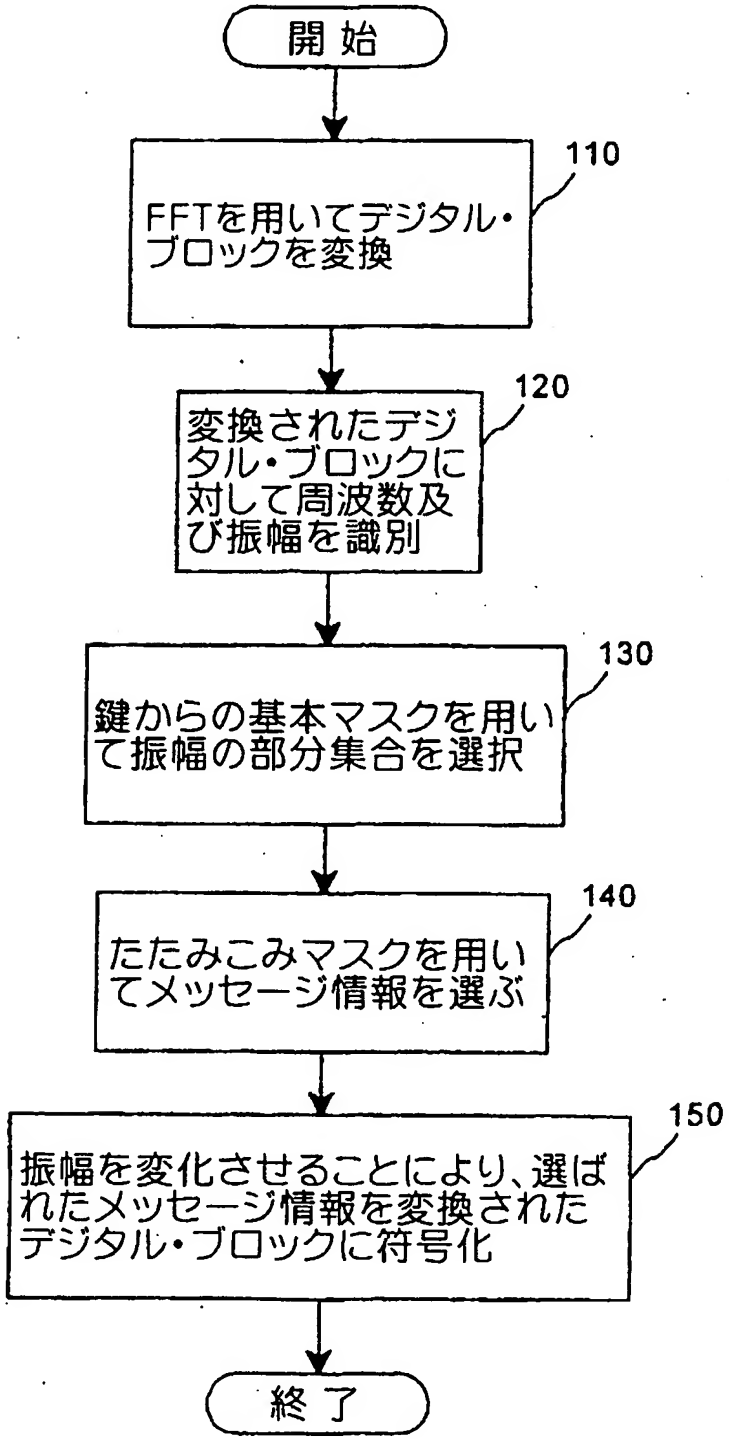
FIG. 2


START
開始
310
Decode Digital Information
デジタル情報を復号化
320
Compare Decoded Amplitudes with Amplitudes in Key
復号化された振幅を鍵の中の振幅と比較
330
Assemble Message
メッセージをアセンブル
340
Hash and Compare with Original Message
ハッシュ化を行い、元のメッセージと比較
350
Declare Results to User
結果をユーザに宣言
END
終了

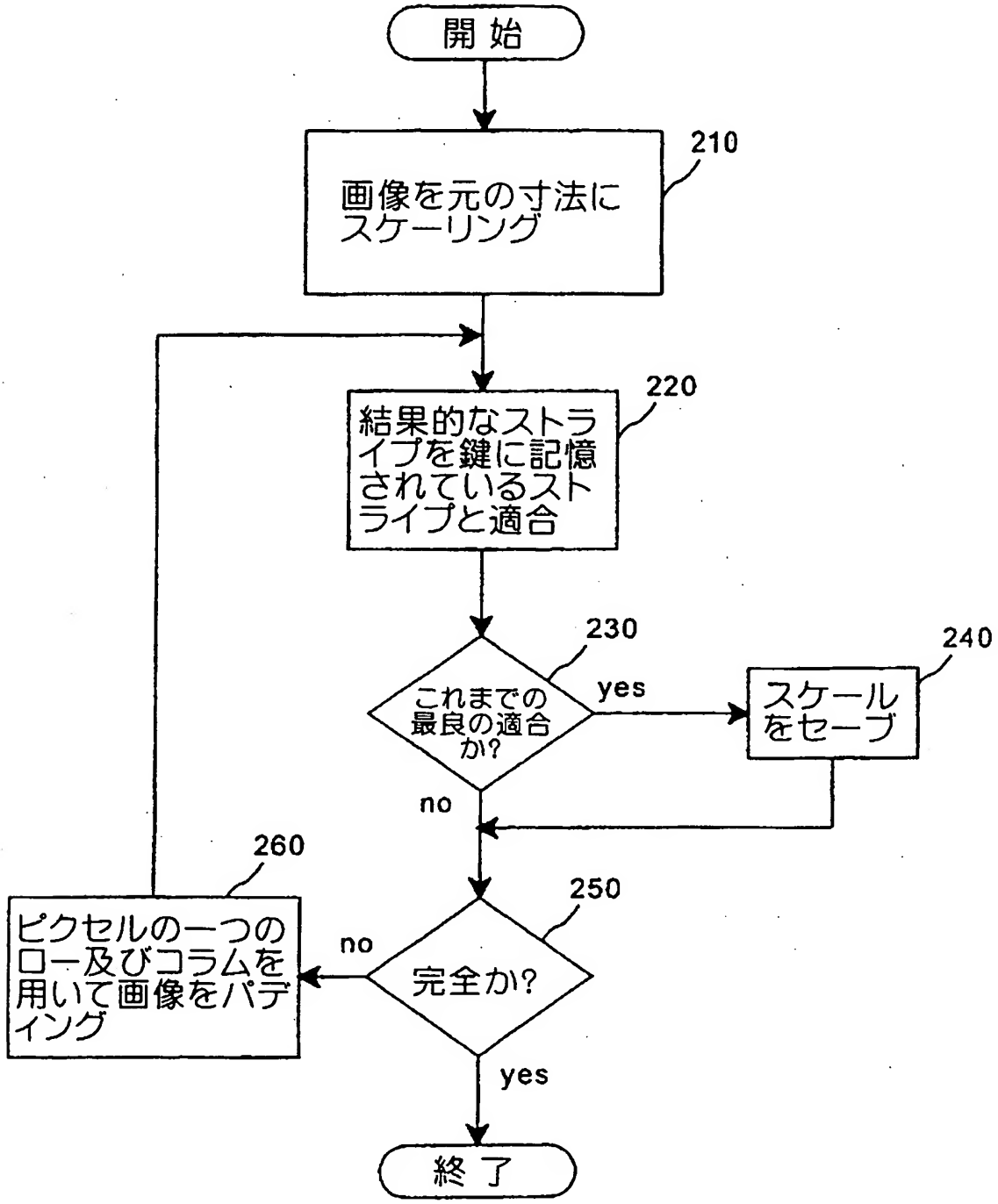
【 FIG. 3 】

【書類名】　　図面

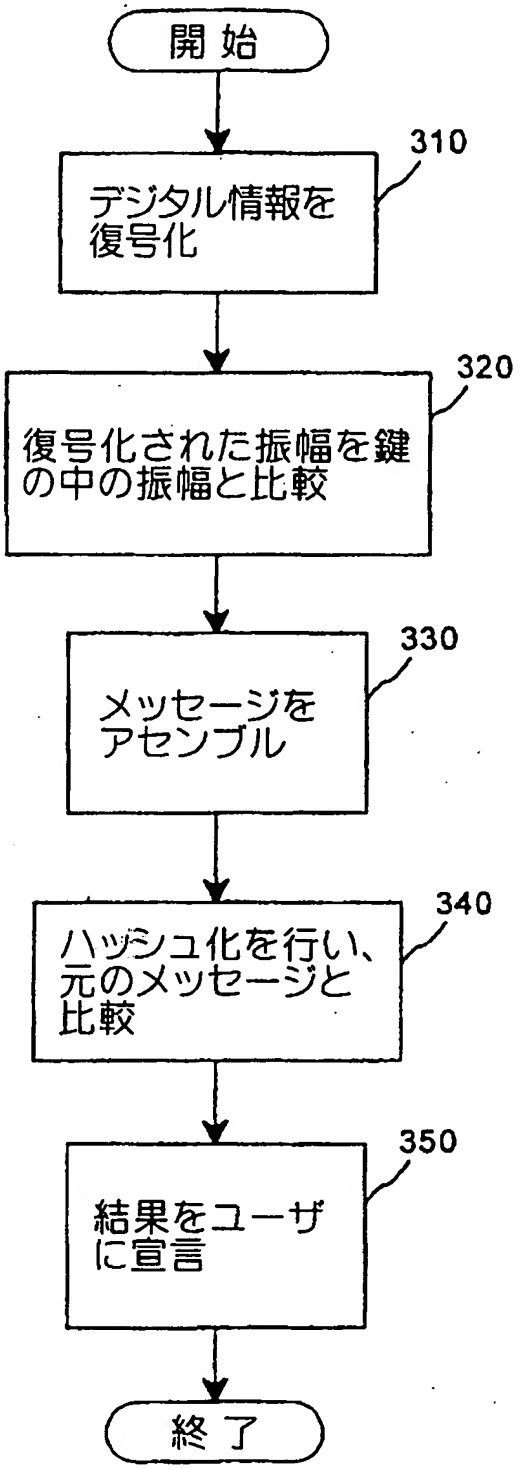
【図１】


開始
FFTを用いてデジタル・ブロックを変換
110
変換されたデジタル・ブロックに対して周波数及び振幅を識別
120
鍵からの基本マスクを用いて振幅の部分集合を選択
130
たたみこみマスクを用いてメッセージ情報を選ぶ
140
振幅を変化させることにより、選ばれたメッセージ情報を変換されたデジタル・ブロックに符号化
150
終了

【図２】


開始
画像を元の寸法にスケーリング
210
結果的なストライブを鍵に記憶されているストライブと適合
220
これまでの最良の適合か?
230
yes
スケールをセーブ
240
no
ピクセルの一つのロー及びコラムを用いて画像をパディング
260
no
完全か?
250
yes
終了

【図３】


開 始
310
デジタル情報を復号化
320
復号化された振幅を鍵の中の振幅と比較
330
メッセージをアセンブル
340
ハッシュ化を行い、元のメッセージと比較
350
結果をユーザに宣言
終 了

【書類名】　要約書

【要約】　安全なデジタル透かしのための複数の変換の利用及び適用である。本発明の或る実施例では、保護されるべきデジタル情報におけるデジタル・ブロックは、高速フーリエ変換を用いて周波数領域に変換される。複数の周波数及び関連する振幅が、変換されたデジタル・ブロックのそれぞれに対して識別され、識別された振幅の部分集合が、鍵からの基本マスクを用いてデジタル・ブロックのそれぞれに対して選択される。メッセージ情報が、畳み込みマスクを用いて発生された変換テーブルを用いて、メッセージから選択される。選ばれたメッセージ情報は、選択されたメッセージ情報に基づいて選択される振幅を変化させることによって、変換されたデジタル・ブロックのそれぞれに符号化される。

【書類名】　手続補正書　Filed: October 13, 2000

【整理番号】　002365I

【提出日】　平成12年10月13日

【あて先】　特許庁長官　殿

【事件の表示】

【国際出願番号】　PCT/US99/07262

【出願の区分】　特許

【補正をする者】

【住所又は居所】　アメリカ合衆国フロリダ州３３１６０，マイアミ，コリンズ・アベニュー　１６７１１，ナンバー　２５０５

【氏名又は名称】　スコット・エイ・モスコウィッツ

【代理人】

【識別番号】　100089705

【住所又は居所】　東京都千代田区大手町二丁目２番１号　新大手町ビル２０６区　ユアサハラ法律特許事務所

【弁理士】

【氏名又は名称】　社本　一夫

【手続補正　1】

【補正対象書類名】　図面

【補正対象項目名】　全図

【補正方法】　変更

【補正の内容】　1

【その他】　浄書につき、図面の実体的内容には変更なし。

【プルーフの要否】　要